Keeping research data of human participants secure, when working with Information Communication Technologies ("ICT")

Introduction

The University through a series of policies and guidelines provides direction and guidance on how data and information are to be handled and protected, when using ICT, to help safeguard individuals and the institution.

This guidance gives advice on how to best use ICT facilities and services to safely work with personal data to support research.

The University Information Classification Policy[1]

The University's information classification scheme has four levels.

Under what classification(s) will research data fall?

Data involving human participants

Research data gathered from human participants will in most instances be personal data. Personal data is any information relating to natural persons who: can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. It may involve details about an identifiable individual's racial/ethnic origins, religious/philosophical beliefs, trade union membership, health details and details of sex life/sexual orientation, which are defined as special categories of personal data.

- Personal data is classified as **CONFIDENTIAL** with special categories of personal data being classified as **STRICTLY CONFIDENTIAL**.

Pseudonymised data

Where research data about human participants has been pseudonymised i.e. the identifying characteristics such as a name have been removed and replaced with a code or codename that can be separately linked by a researcher to that individual, those data still fall within the scope of personal data for the purposes of European and UK data protection law.

When working with pseudonymised data the University still has responsibility to protect individuals' personal data, however there can be more flexibility when working with that data on a range of ICT devices, because privacy risks are reduced.

When working with pseudonymised data the means of deciphering the code or codename to understand the names/identities of the participants must be held separately and securely from the pseduonymised participant data.

Anonymised data

This is data that has been rendered irreversibly anonymous i.e. all identifying features have been permanently removed, and the data cannot be reconstituted to identify individuals. Therefore anonymised data does not constitute personal data.

[1] Available from: https://www.st-andrews.ac.uk/itsupport/security/classification/

What ICT devices and storage services, including cloud based, can I use?

The following guidance is for data classed as CONFIDENTIAL and STRICTLY CONFIDENTIAL.

University ICT devices

It is preferable to make use of ICT devices that has been procured by the University via IT Services; those items in most instances will have the relevant:

- Antivirus and anti-spyware/malware software necessary to protect a device and any information stored; and
- Encryption, supported with central key management (– if you lose/forget the password, a secure lost/forgotten password facility is available through the University IT Service Desk, who can arrange for a password reset).

If you are unsure whether a University device is suitably protected or otherwise, please ask a School Computing Officer or contact the IT Service Desk.

If using a Dictaphone to record interviews or a video camera, you should work with a device that is capable of being encrypted; should a device become lost or stolen, without the password third parties will not be able to access and make use of the interview materials.

What options do I have, if I cannot work with the arrangements noted above?

You should take the following steps, so that you are working with data in a format that does not readily identify the persons concerned:

- Can you work with research data in such a way that the data is anonymous? If anonymous then if the data were to become lost, stolen or compromised in any way then there no risk the privacy and safety of the research participants;
- If anonymisation is not possible, only use research data in a pseudonymised form e.g. instead of identifying a person by name, make use of a research participant number or codename;
- The details that link the code or codename to named participants must be held securely on a separate device preferably those details will be stored on the University network or as an alternative an encrypted device; and
- Consider what data do you need to work with on an unsecured device? Do you need all the data, or can you make use of a sub-set at a point in time?

Storing research data

Storing files on a device such as a PC, Laptop or USB stick with no means of separate backup is risky. Technology routinely fails; files can become corrupted and unreadable putting materials beyond use. Human error can lead to files being accidently deleted, and devices can be lost or stolen.

It is preferable to store all research data on the University network; this provides a high degree of security and protection. Backup copies of files stored on the University network are regularly made.

Of course, there will be times when you collect data which cannot be directly saved/stored on the University network. In those instances, it is recommended that files are securely transferred to the University network at the earliest opportunity.

Working with portable storage devices

When working with laptops, USB sticks and other forms of portable storage, the data must be encrypted to the standard AES 256, with the facility for key management (secure password reset) being available should you lose/forget the password. When working with laptops specifically, they must be configured with antivirus and anti-spyware/malware software and to apply the latest operating system updates as they become available.

Transferring files

It is important to be mindful how to transfer files securely so that the confidentiality of research participants is maintained. When working away from the University, if you will have access to the University network, via VPN, then accessing the materials you require remotely, from source is recommended. This is secure and once saved on the network the materials will be backed-up during the next scheduled cycle. Alternatively, save copies of the files you require onto an encrypted device (see above).

When sharing files with colleagues at other institutions:

- If using email, please email from the University account to the work/official account of the colleague(s)/partner(s). If data/materials are being shared in identifiable form, then password protect/encrypt the file before sending as an email attachment; or
- Consider making use of Office 365 or SharePoint to set up a secure area where others can access to view and retrieve materials.

Passwords

When working with ICT, passwords are often the first and last line of defence to protect information from becoming available to others, who have no right of access. It is essential that University guidelines on selecting and working with Strong Passwords are followed: https://www.st-andrews.ac.uk/strongpasswords/

In line with the University ICT Regulations passwords and other security credentials must never be shared or transferred.

Cloud storage

European and UK data protection laws place restrictions on how organisations work with third parties to manage/process personal data, cloud service providers being a notable example. The legislation requires that before a third party is engaged to provide services that specific contractual terms exist between both parties; before such an agreement can be reached, a level of due diligence is required.

In terms of cloud storage provision, to date, the University has only undertaken due diligence with Microsoft for the provision of Office 365 and SharePoint cloud-based storage. This means that presently the services of other providers such as Box cannot be used to store personal data or special categories of personal data concerning human participants.

Microsoft Office 365 applications and files can be synchronised across several devices, which could include a portable storage device. Microsoft Office 365 Cloud services can only be used to store research participant data classified as either CONFIDENTIAL or STRICTLY CONFIDENTIAL where those data would be synchronised portable storage devices that meet the requirements set out above.

Other considerations

Data are often processed on applications/services that are not owned or operated by the University. Before data involving human participants can be used with third-party services data protection law requires that several checks take place: to ensure that there are no information security vulnerabilities and that a specific 'data processor' contract is in place, which provides assurances as to how personal data will be managed and protected. If use of applications/services that are not currently provided by or through the University are required to manage human participant research data, then in the first instance an email to the IT Service Desk will start the discussion about how we can support this securely.

Reporting a personal data breach

If it is suspected or discovered that personal data have become lost, stolen or compromised in any other way then email dataprot@st-andrews.ac.uk or contact the IT Service Desk.

Further guidance

- University Information Classification policy and implementation guide: https://www.st-andrews.ac.uk/itsupport/security/classification/
- University ICT Regulations:
- https://www.st-andrews.ac.uk/media/library/documents/Regulations%20University%20ICT%20facilities.pdf
- University Research Data Management Policy: https://www.st-andrews.ac.uk/staff/policy/research/researchdata/

Further help

- The University Data Protection Officer: email dataprot@st-andrews.ac.uk
- University of St Andrews Computer Security Incident Response Team: email stacsirt@st-andrews.ac.uk
- University of St Andrews IT Service Desk: email itservicedesk@st-andrews.ac.uk
- Research Data Management: email research-data@st-andrews.ac.uk
- University Teaching and Research Ethics Committee (UTREC): email utrec@st-andrews.ac.uk
- Research and Innovation Services: email rpo@st-andrews.ac.uk